UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,377	12/20/1999	YURIJ ANDRIJ BARANSKY	Y0999-558	3573

7590 07/12/2004

DOUGLAS W CAMERON
INTELLECTUAL PROPERTY LAW DEPT
IBM CORPORATION P O BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,377	BARANSKY ET AL.	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending.

2. Amendment submitted 20 May 2004 has been received and entered.

Response to Arguments

3. Applicant's arguments filed 20 May 2004 have been considered, but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 5-7, 12-13, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mi et al US Patent No. 6,418,472 in view of Olden US Patent No. 6,460,141 and Aziz US Patent No. 5,604,803. Mi teaches a system and method for using Internet based caller ID for controlling access to an object stored in a computer. Olden teaches a security and access management system. Aziz teaches a method for secure remote authentication in a public network.

6. With regards to claims 1,12, and 15, Mi teaches the generating of a first key known only to the content provider (Mi, column 7 lines 21-27, column 8 lines 47-61), the

encrypting of a second key using the first key and an encryption algorithm (Mi, column 8 lines 4-10, column 4 lines 21-28), decrypting the second key using the first key when the user desires access to data (Mi, column 8 lines 32-46), and accessing the data using the second key (Mi, column 8 lines 32-46). Mi lacks a reference to the use of a one-time password and the storing of the encrypted second key on the client machine. Aziz teaches the use of a one-time password (Aziz, column 6 lines 61-64) and Olden teaches the storing of an encrypted second key on the client machine (Olden, column 23 line 55 – column 24 line 28 "cookie"). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Olden's method of storing an encrypted cookie on a client machine and Aziz's method of using one-time passwords with Mi's access control system because it offers the advantage of relieving the user of the hassle of having to enter authentication information each time access is requested to a service or object (Olden, column 23 lines 55-61) and because it reduces the likelihood of an unauthorized user gaining access to user passwords (Aziz, column 2 lines 1-13).

7. With regards to claims 2 and 6, Mi as modified discloses the step of transmitting the identity of the client machine to the content provider to authenticate that the user is using the client machine thereby permitted data to be accessed only on the client machine (Mi, column 8 lines 32-46).

8. With regards to claims 3 and 7, Mi as modified teaches the one-time password being a unique user identifier and the one time password being transmitted out of band (Aziz, column 2 lines 45-60).

9. With regards to claims 5, 13 and 16, Mi teaches everything as described above, and further teaches the use of a separate user supplied password (Mi, column 8 lines 14-19).

10. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over over Mi et al US Patent No. 6,418,472 in view of Olden US Patent No. 6,460,141 and Aziz US Patent No. 5,604,803 as applied to claims 1 and 5 above, and further in view of Thomlinson et al US Patent No. 6,389,535.

11. With regards to claims 4 and 8, Mi as modified fails to teach the second key being required in an algorithm that generates a session key used to decrypt data. Thomlinson teaches a second key being required in an algorithm that generates a session key used to decrypt data (Thomlinson, column 10 lines 11-16). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Thomlinson's method of session key creation with Mi as modified because it offers the advantage of allowing encryption of secret data in such a way as to ensure that data items don't need to be re-encrypted when a user changes his or her password (Thomlinson, column 10 lines 17-23).

12. Claims 9-11, 14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mi et al US Patent No. 6,418,472 in view of Olden US Patent No. 6,460,141, Aziz US Patent No. 5,604,803, and Jablon US Patent No. 6,226,383 in view

of Thomlinson et al US Patent No. 6,389,535. Jablon describes cryptographic methods for remote authentication.

13. With regards to claims 9, 14, and 17, Mi teaches the generating of a first key known only to the content provider (Mi, column 7 lines 21-27, column 8 lines 47-61), the encrypting of a second key using the first key and an encryption algorithm (Mi, column 8 lines 4-10, column 4 lines 21-28), decrypting the second key using the first key when the user desires access to data (Mi, column 8 lines 32-46), and accessing the data using the second key (Mi, column 8 lines 32-46). Mi lacks a reference to the use of a one-time password, the storing of the encrypted second key on the client machine, the sending of g^a to the client machine, generating g^b, encrypting g^b, and calculating g^(a*b) as part of the authentication procedure. Aziz teaches the use of a one-time password (Aziz, column 6 lines 61-64) and Olden teaches the storing of an encrypted second cookie on the client machine (Olden, column 23 line 55 – column 24 line 28 "cookie"). Jablon teaches a procedure called Hidden-Password Validation that includes the sending of g^a to the client machine (Jablon, column 7 lines 16-23), generating g^b (Jablon, column 7 lines 23-26), encrypting g^b (Jablon, column 7 lines 23-26 g^b is exchanged using Diffie-Hellman encryption), and calculating g^(a*b) (Jablon, column 7 lines 25-27) as part of the authentication procedure. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Olden's method of storing an encrypted cookie on a client machine, Aziz's method of using one-time passwords, and Jablon's exchange procedures with Mi's access control system because it would offer the advantage of relieving the user of the hassle of

having to enter authentication information each time access is requested to a service or object (Olden, column 23 lines 55-61), because it would reduce the likelihood of an unauthorized user gaining access to user passwords (Aziz, column 2 lines 1-13), and because it would help reduce the vulnerability of the password if a host computer's password database is exposed (Jablon, column 20 lines 17-20).

14. With regards to claim 10, Mi as modified discloses the step of transmitting the identity of the client machine to the content provider to authenticate that the user is using the client machine thereby permitted data to be accessed only on the client machine (Mi, column 8 lines 32-46).

15. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mi et al US Patent No. 6,418,472, Olden US Patent No. 6,460,141, Aziz US Patent No. 5,604,803, and Jablon US Patent No. 6,226,383 as applied to claim 9 above, and further in view of Schneier Applied Cryptography. Mi as modified, lacks a reference to a MAC authentication procedure. Schneier describes the one-way hash function termed a MAC that is used to verify authenticity (Page 455, Section 18.14). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's MAC authentication on g^{a*b} to authenticate the server to the client because it provides a verification method that is reliant on having the same key. Both client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security since it is a one-way function (Page 455, Section 18.14).

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137